

8. The method of claim 1, wherein the facial image data comprise a three-dimensional facial image of the subject.

9. The method of claim 1, further comprising:

downloading by a web crawler facial images of individuals and personal information associated therewith; and storing the downloaded facial images and associated personal information in the database.

10. The method of claim 9, wherein the reference facial recognition data comprise the facial images downloaded by the web crawler or the facial images obtained from the Internet, professional websites, law enforcement websites, or departments of motor vehicles.

11. The method of claim 1, wherein the database comprises a plurality of criminal records associated with the facial images stored in the database.

12. The method of claim 1, wherein the facial recognition data comprise a vector representation of the captured facial image of the subject and the reference facial recognition data comprise a vector representation of the stored facial image in the database.

13. The method of claim 12, wherein the vector representation of the captured facial image of the subject or the vector representation of the stored facial image in the database comprises a 512 point vector or a 1024×1024 facial data matrix.

14. The method of claim 12, wherein the step of comparing further comprises comparing the vector representation of the captured facial image of the subject to the vector representation associated with the stored facial images in the database.

15. The method of claim 1, wherein comparing the facial recognition data is performed by a machine learning module.

16. The method of claim 15, wherein the machine learning module comprises a deep convolutional neural network (DCNN).

17. The method of claim 1, wherein identification of the candidate is performed by the k-nearest neighbors algorithm (k-NN).

18. The method of claim 1, further comprising detecting a liveness gesture.

19. The method of claim 18, wherein the liveness gesture is based on at least one of a yaw angle of a second image relative to a first image and a pitch angle of the second image relative to the first image, wherein the yaw angle corresponds to a transition centered around a vertical axis, and wherein the pitch angle corresponds to a transition centered around a horizontal axis.

20. The method of claim 1, wherein the personal information is retrieved from the database based on a predetermined privacy setting of the identified candidate.

21. The method of claim 1, further comprising displaying one or more facial images of the identified candidate and the personal information associated therewith.

22. The method of claim 1, further comprising transmitting a notification to the user device if the identified candidate poses a high risk to the public or is a criminal.

23. The method of claim 1, wherein the personal information comprises a name of the identified candidate or a link to an online profile associated with the identified match.

24. The method of claim 1, wherein the personal information transmitted to the user device is obtained from a webpage having the highest PageRank value among the webpages containing the personal information.

25. The method of claim 1, further comprising:

determining a permission of access for the subject to a venue or an account based on the personal information of the identified candidate;

granting the access for the subject if the identified candidate is an authorized user, or

denying the access for the subject if the identified candidate is not an authorized user or a candidate matching the captured facial image cannot be identified; and

transmitting a message indicative of granting or denying the access to the venue or the account.

26. The method of claim 25, comprising providing access to the database to a plurality of users.

27. The method of claim 1, wherein the facial image data comprise a second captured facial image of a second subject.

28. The method of claim 27, further comprising identifying a relation between two or more subjects having facial images captured in a single image.

29. A method of verifying an identity of a user, comprising:

providing a facial image data comprising a captured facial image and a personal identification number of the user; transforming the facial image data to facial recognition data;

comparing the facial recognition data and the personal identification number to reference facial recognition data and reference personal identification numbers associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image and the personal identification number; and

upon identification of the candidate, transmitting a confirmation to a user device indicating the user is an authorized user.

30. A system for providing information about a subject, comprising:

a facial image processing module operable to transform a captured facial image of the subject to a facial recognition data; and

a facial recognition module operable to:

compare the facial recognition data to reference facial recognition data associated with a plurality of stored facial images of individuals to identify at least one likely candidate matching the captured facial image,

upon identification of the candidate matching the captured facial image, retrieve from the database personal information associated with the candidate, and

transmit the personal information to the user device and cause the user device to display the personal information.

\* \* \* \* \*